AIR WAR COLLEGE

AIR UNIVERSITY

DIGITAL DATA WARFARE:

USING MALICIOUS COMPUTER CODE AS A WEAPON

by
Lawrence G. Downs Jr.
Commander, USN

A RESEARCH REPORT SUBMITTED TO THE FACULTY

IN

FULFILLMENT OF THE CURRICULUM

REQUIREMENT

Advisor: LTC James R. Brungess

MAXWELL AIR FORCE BASE, ALABAMA

April, 1995

DISCLAIMER

This study represents the views of the author and does not necessarily reflect the official opinion of the Air War College or the Department of the Air Force.

Loan copies of this document may be obtained through the interlibrary loan desk of the Air University Library, Maxwell Air Force Base, Alabama 36112-5564 (telephone [334] 953-7223 or DSN 493-7223).

ABSTRACT

TITLE: Digital Data Warfare: Using Malicious Computer Code as a Weapon

AUTHOR: Lawrence G. Downs Jr., Commander, USN

Digital Data Warfare (DDW) is an emerging field that has great potential as a means to meet military, political, economic or personal objectives. Distinguished from the "hacker" variety of malicious computer code by its predictable nature and the ability to target specific systems, DDW provides the attacker with the means to deny, degrade, deceive and/or exploit a targeted system. The five phases of a DDW attack--penetration, propagation, dormancy, execution and termination--are presented for the first time by the author in this paper.

The nature of DDW allows it to be used in the strategic, operational and tactical warfare roles. Three questions should be considered when developing a strategy for employing DDW: (1) Who should control the employment of DDW? (2) What type of systems should be targeted, and (3) Under what circumstances should DDW be used?

Finally, a brief overview of possible countermeasures against DDW is provided as well as an outline of an effective information system security program that would provide a defense against DDW.

Digital Data Warfare: Using Malicious Computer Code as a Weapon

John Gantz's April 1, 1991 column in *InfoWorld* described a new and awesome weapon: a software virus developed by the best programmers at NSA to target real-time computer systems. Dubbed AF/91, the virus is designed to exploit highly protected command and control systems through their less protected peripheral interfaces. Once inside, a neural network component of the virus adapts the virus to work within virtually any architecture. It reportedly takes the neural network a couple of weeks to get set up on a system that runs 24 hours a day (setup time is directly related to machine cycles), but once complete is able to put the entire system out of commission. Gantz reported that AF/91 was installed by the CIA onto a printer that was smuggled into Iraq and subsequently used with Iraqi air defense systems during the Gulf War. More than half of the displays and printers used by the Iraqi air defense system were disabled. The result is history. It is not until the final paragraph that Gantz lets the reader in on the joke. AF/91 gets its name from the fact that 91 is the Julian Date for April Fool's Day.[1]

Although the above scenario is fictional, the state of technology today makes the concept of using malicious computer code as a weapon very real. It is now possible to develop computer software viruses that target specific systems, install the viruses covertly and then have them operate in a manner that is advantageous and predictable to the attacker. There are no published incidents of computer viruses being used as a military offensive weapon in open source literature, but such attacks are not only feasible, but probable.

What is Digital Data Warfare?

Digital Data Warfare (DDW) is malicious computer code covertly introduced into one or more specific computer systems or networks, by an attacker to meet military, political, economic or personal objectives. The objective may be tangible (financial gain) or intangible (a political statement) but is more than just the satisfaction of having written the code itself. Unlike other

[1]Gantz, John. "Meta-Virus Set to Unleash Plague on Windows 3.0 Users." InfoWorld 13 (01 April 1991): 39.

types of malicious code, DDW code is a tool--a means to an end--not an end in itself. It is one of the many weapons an information warrior may use to ply his trade.

DDW may take the form of a virus, worm, logic bomb, time bomb, trojan horse, or some combination,[2] depending on its function, but it differs from the "hacker" variety of these insofar as it targets a *specific system* (or network of systems), for *a specific objective*, in a manner that is *predictable to the attacker*. Within this definition, the attacker could be a military or national organization, a terrorist organization, a multi-national or private corporation, or even an individual with the knowledge and means to produce and install such code. Some examples that serve to depict the breath of DDW are shown in table 1 below:

Attacker	Specific Target	Specific Objective	Ultimate Goal
Military or National Organization	Enemy C4I Network	Disrupt Command and Control of enemy units	Win the War
Terrorist Organization	AT&T Telephone Computer System	Interrupt business activities, financial transactions and flow of information	Make a Political Statement
Private Corporation	Competitor's R&D Database	Gain access to proprietary information	Gain a Competitive Advantage
Disgruntled/Dishonest Employee	Company's Accounting System	Transfer money to a bogus account long after employee departs	Financial Gain and/or "Punish" Company

Table 1 - Examples of Digital Data Warfare

DDW is not as farfetched as many would believe. While the use of DDW by military and national organizations, terrorist organizations or corporations has not yet been confirmed in the open press, there have already been documented cases of DDW being used by individuals in the private sector for personal gain. One such instance is described by John Dehaven, a computer security expert:

> "I once helped investigate a software time bomb that had been planted in the accounting system of a large corporation. Months before certain employees left the company (and the country), they planted a time bomb

[2]See Appendix I for a definition of these terms.

> programmed to produce a fake invoice that was due and payable. The bill had all the authorizations necessary to satisfy the accounts-payable system, and it was for an amount that didn't require authorization. On the appointed day, the firm's computer automatically transferred the money to a bogus vendor's account in a Swiss bank. The perpetrators withdrew the cash from the bank, left Switzerland, and are still at large."[3]

While it is easy to dismiss such an incident as a fluke, unlikely to have far reaching or serious effect outside its immediate domain, consider the fact that microcomputers have only been in widespread use for fifteen years and the number of persons capable of authoring such complex computer code in the past was limited. The growing sophistication of high school students now entering college will ensure an ever greater pool of persons capable of writing such viruses. One college professor related an experience he had when he addressed a group of high school students on computer viruses:

> "As I described the different portions of the system that should be protected against viruses - for example, boot sector, interrupt sector and so on - one of the students interjected, 'Well, if you're doing all that, I could still penetrate the video portion of the system.'
>
> "If 16-year-old kids are spontaneously coming up with ideas on how to subvert viral protection methods, you can just imagine what we're in store for in the future."[4]

Although DDW is a field whose promises and complexities are still being studied in depth, the design and operation of DDW computer code is now within the state-of-the-art.

Digital Data Warfare Objectives

An attacker using DDW seeks to affect the targeted system in one or more of the following ways:

Denial - deny the intended target the use of the system, its data, or the information it provides. This can be done using malicious code that cause hardware failures or the destruction of programs and data.

---

[3]Dehaven, John. "Stealth Virus Attacks." Byte 18.6 (1993): 137.
[4]DiDio, Laura. "A Menace to Society." Network World 06 February 1989: 82.

Degradation - degrade the targeted system to the point where it cannot effectively perform its mission. This can be accomplished by forcing the target to remove the infected unit from the rest of the network for fear of causing a more widespread infection or by introducing a worm that overloads the processing capabilities of the system.

Deception - deceive the targeted system into generating false information or into believing that erroneous data is actually accurate.

Exploitation - provide a means by which information on the targeted system can be transmitted back to the attacker.

The objectives of DDW depend upon the attacker and his intentions. A terrorist organization would probably be most interested in accomplishing the first two objectives: denial and degradation. A corporation may be only interested in exploitation. For the military, attaining all the listed objectives are important, though not necessarily in every case. Each attacker must evaluate his own needs and technical abilities prior to developing a strategy for using DDW.

Phases of a DDW Attack

DDW attack consists of a series of steps that are accomplished in a predetermined sequence. As mentioned earlier, the DDW code may be a virus, worm, logic bomb, time bomb, trojan horse or some combination of these. The term "DDW code" will be used to refer to all these collectively. "Virus," "worm," and so forth, will be used when it is necessary to specifically identify the type of code being referred to. The phases of a DDW attack are as follows:

- Penetration Phase

  DDW code is inserted into the system, usually through its weakest link.

- Propagation Phase

  The DDW code propagates through the system to find the intended target.

- Dormancy Phase

  The DDW code maintains covertness until triggered into action.

- Execution Phase

The DDW code is triggered into action and performs the steps necessary to deny, degrade, deceive or exploit the system.

• Termination Phase

Once the objectives have been accomplished, the DDW code can either return to the dormancy phase for a future attack or erase itself throughout the system in order to leave no trail.

Penetration Phase

Implanting the computer code into the target system is probably the most challenging phase of employing DDW. There are two aspects that must be considered: the point of penetration and the method of penetration.

Point of Penetration. The code can be implanted directly into the target system (direct penetration), or it may be inserted into a peripheral or less protected node and then be designed to propagate to the intended target (indirect penetration). In many cases the target system is well protected to stand up against a direct DDW assault, so more often than not the attacker is forced to enter a less protected part of the system.

Method of Penetration. Cramer and Pratt describe the two options as "front-door coupling" and "back-door coupling."[5]

Front-door coupling is defined as accessing the target by using media for which it was designed. Inserting a computer disk into a floppy drive or directing radio waves at a receiving antenna are examples of front-door coupling. During front-door coupling, the DDW code generally takes the form of a trojan horse hidden within legitimate computer code.

Back-door coupling is any technique used to access the target system by media other than the one for which the system was designed.[6] This can be done through power or stability systems,

[5]Cramer, Myron L. and Pratt, Stephen R. "Computer Virus Countermeasures - A New Type of EW." Defense Electronics October 1989, 80.

[6]Ibid.

high energy radio frequency application or, more promisingly, through carefully controlled electromagnetic pulses. The Defense Department is reportedly considering developing viruses to insert into the EPROMs of US manufactured weapons in case they fall into the wrong hands.[7] This trojan horse program would be enabled by sending an enciphered RF code. One particularly ingenious method suggested by Cramer and Pratt is to design an infected processor and take advantage of "the almost blind replication of processors into hostile systems" to get the enemy to unknowingly place DDW computer code into his own system.[8]

Front-door and back-door coupling can be used in conjunction with either direct or indirect penetration. Table 2 below gives examples of this:

	Direct Penetration	Indirect Penetration
Front-Door Coupling	DDW code is inserted directly into a payroll system by a trusted user utilizing a terminal.	DDW code is transmitted via RF up an unprotected aircraft data link which in turn unknowingly transmits the code to the Command Center (target) during encrypted communications.
Back-Door Coupling	A coprocessor with DDW code is included in shipment to competitor and subsequently installed onto main network system board.	Sophisticated terrorists use electro-magnetic pulses to insert DDW code into power company's computers, eventually bringing down the city's power grid.

Table 2 - Examples of How DDW Code Can Be Inserted Directly or Indirectly Using Front-Door and Back-Door Coupling

Propagation Phase

Once the DDW code has penetrated the system, it next must propagate through the system and locate its intended target. The target may be all the components of the system or just one piece of data. The target can be software or hardware. It can be the main file server or a node. The key here is for the attacker to carefully consider his objectives and determine exactly

[7]Madsen, Wayne. "Government-Sponsored Computer Warfare and Sabotage." Computers & Security 11.3 (1992): 234.

[8]Cramer, 82.

what the target is. If the code had been inserted directly, it is already in the target system and must now locate a place to lie undetected until the execution phase.

In many cases, it would be a mistake to design DDW code that would infect all the components of a system if the attacker's goal is achievable by only infecting one piece of that system. The DDW designer needs to minimize the opportunity for the target to detect the code. A virus that has spread throughout the entire system is more apt to be detected, and once found, is less apt to succeed in its mission. At times it may be necessary to search all the components of a system to find the intended target, but once the target is found or a dead end to a search path is detected, the code should erase itself where it is not needed.

Dormancy Phase

Once the code has located the target, it can lie dormant until it is time to attack. In some cases the timing of the attack is unimportant and would immediately follow infection, such as a worm designed to bring down the TeleCheck network or a virus designed to destroy payroll files. In most cases, however, the timing of the attack is crucial to meeting the attacker's overall goals. A military organization employing DDW would want to ensure the enemy's C4I network is disabled just prior to an offensive. A terrorist group may want the attack to coincide with a particular event or occur during a particular time of the day. A dishonest employee would want to be long gone before a virus he inserted was triggered. One of the advantageous properties of DDW is that weeks, months or even years can elapse between the time the code is introduced into a system and the time it is triggered. This characteristic makes it extremely difficult to determine where and how it penetrated the system. More importantly, irreparable damage may have been incurred long before discovery and a response may be all but impossible.

DDW code can also remain dormant within a system for its entire life and never be called upon to accomplish its mission. It can lie in wait for an external trigger and if the system in which it is resident is never targeted for an attack, the trigger is never activated. In this case, DDW is

inserted into a system as a hedge against future contingencies and not in contemplation of a specific attack.

The dormancy phase lasts until the code is pressed into service by the triggering mechanism.

The Execution Phase

The execution phase begins when the triggering mechanism activates the code from its dormant state. DDW code may trigger into action at a certain time and date as read from the system's clock or it may go into action after executing a certain number of machine cycles. Some viruses will trigger their mission component as soon as they propagate to the part of the system they are designed to attack. Other triggering mechanisms include: the transmission of a certain RF signal; the logon of a specific bogus account name; and, even the entry of certain predetermined valid data (for example, a landing request from aircraft callsign XYZ 123 could trigger a virus in the air traffic control system).

Sometimes DDW code acts right away and does not require a triggering mechanism. In the case of a DDW worm designed to bring down the TeleCheck network, for example, the code would replicate itself throughout the system until it overloads the system's processing capabilities and degrades the system to a level desired by the attacker. Such a worm would go to work immediately upon penetration, would not lie dormant at anytime throughout its life, and therefore would not need a triggering mechanism.

Once triggered, the DDW code springs into action and performs its primary objective: denial, degradation, deception and/or exploitation.

Denial. The DDW code can deny the target the use of his system in a variety of ways. By far the easiest is to destroy the target's data and/or application programs. Other types of DDW code could attack the hardware components of a system. For instance, a virus that could jiggle the clock rates of critical computer chips could cause the chips to heat up to a point where

they would self-destruct.[9] DDW code could also attack the dynamic components of the system, introducing stresses for which they were not designed, such as continually and repeatedly moving hard drive read/write heads back and forth until failure. A virus could also remove a software limitation on a hardware component of the system that would induce hardware failure when the component is pressed into service beyond its design limits.

Degradation. As mentioned earlier, a worm introduced into a system could overload the system's resources to the point where the system could not effectively do the job for which it was intended. The famous 1988 Internet worm demonstrated the effectiveness of this.[10] In that attack, up to 6,000 machines connected to the world-wide network crashed just twelve hours after the introduction of the worm, bringing traffic on the net to a near halt. Yet, a virus does not have to overload the system in order to degrade it. Just the fear that a component of a system may contain a virus is often justification enough to bring down the system and have it thoroughly checked. During the 1993 Michelangelo virus scare, countless dollars and man-hours were expended in looking for the virus while only a few instances of it were ultimately discovered. According to Mario Discepola, vice-president of ND Computer Resources Ltd., this type of threat is "costing us hundreds of millions of dollars."[11] One recent survey of Fortune 1000 companies indicated costs of $30,000 per hour of LAN downtime, based on lost productivity and revenue, and direct expenses.[12]

Even if the whole system is not brought down, the fear that a particular component of a system is infected may be enough to have that component removed from the system in order to avoid the risk of further contamination. The degradation caused by the removal of that component from the system may be enough to meet the objectives of the attacker.

---

[9]Alexander, Michael. "Military Sees Problems, Promise in Viral Strikes." Computerworld 08 April 1991, 97.
[10]Fisher, Sharon. "The Internet Worm Celebrates Its First Birthday." InfoWorld 23 October 1989, S10-S12
[11]Jenish, D'Arcy. "A 'Terrorist' Virus." Maclean's 16 March 1992, 51.
[12]Preston, Charles. "Creating a Corporate Virus Plan." Computers & Security 10.8 (1991): 701.

Another form of degradation that is being studied is called "psycho-electronics." Here, a virus introduced into the system causes the video screen to flicker imperceptibly, triggering headaches in unsuspecting radar screen operators and others who use the displays.[13]

Deception. One form of deception is allowing the target system to perform the functions for which it was designed while inducing it to treat erroneous data as valid. A small modification to the VISA credit card verification program by a trusted employee could induce the system to treat certain non-valid credit card numbers as valid, allowing the employee and his associates to effortlessly skim off thousands of dollars in merchandise. Though the problem of inserting false data into military systems is far more difficult, the payoffs are even greater. The advantage of having air contacts displayed where there are none and no air contacts where ones actually exist allows for tactical surprise--an edge whose value cannot be overstated.

Another form of deception is covertly changing the workings of the application program while it still appears to be operating as designed. A terrorist organization that inserts DDW code into a hospital system that modifies the workings of the life support computers could turn those systems into lethal weapons. A virus inserted into an ESM system could cause that system to ignore incoming signals of a certain frequency or wave type and still allow that system to test good and appear to be functioning normally.

The modifications to the targeted program do not necessarily have to be extensive. Changing a simple "<" to ">" may very well meet the attacker's objectives. Consider a fire control system whose main program had been modified by DDW code to tell the system to ignore incoming objects going *faster* than 750 knots instead of *slower* than 750 knots. Such a system would not engage incoming missiles as it was designed to but rather it would fire on friendly subsonic aircraft who thought they were in a safe envelope.

Exploitation. Exploitation involves getting specific information from the targeted system back to the attacker. The ease in which this can be accomplished is directly related to how much

[13]Alexander, "Military sees Problems...", 97

access the attacker has to the targeted system. If the attacker has any access at all to the targeted system, the DDW code can store the needed information in any number of places accessible to the attacker. If the attacker is an outsider, the problem is more difficult but, as John Dehaven explains, is not insurmountable:

> "For an outside intruder, any covert communications channel can be used to send signals, because even seemingly random signal sequences can contain an embedded message to someone who knows how to read them. For example, if there are rules to prevent signals from being transmitted from the system to the outside world, an intruder can use an alternating pattern of violation/no violation of the rules like Morse code to send messages.
>
> "An attacker needs only to subvert a network's log-in machinery to erect a reporting mechanism..."[14]

As computer systems become increasingly interconnected, the potential for DDW exploitation becomes ever greater. The Dutch hackers that allegedly penetrated the Department of Defense computers at 34 sites in April and May 1991 were able to modify and copy information linked to military operations in the Persian Gulf.[15] Though that was not an instance of a DDW attack, it illustrates how system administrator and privileged accounts can be created by uncleared persons halfway around the world with no legitimate access to the system. It is also interesting to point out that these hackers were just randomly rummaging through various systems to see what they could find. They had no specific objective in mind and had little knowledge of the systems they were infiltrating. It is easy to imagine what a focused DDW attack could have done.

Termination Phase

Depending on the overall goal of attacker, the DDW code used for the attack may be programmed to destroy all copies of itself after the objectives have been met. Doing this accomplishes several things:

---

[14]Dehaven, 142.

[15]Alexander, Michael. "Poor Security Made DoD Easy Hacker Prey." Computerworld 25 November 1991, 92

- If the attack was not apparent to the target, such as might be the case with exploitation and certain deception attacks, removing the DDW code leaves the target with no clue to why the machine appeared to malfunction (deception) or any evidence that sensitive information may have been disclosed (exploitation).

- In the case where the target knew he was a victim of DDW but was unsure about the nature of the attack, removing the code makes it much more difficult for the target to determine the scope of the attack and the extent of his losses.

- Even where the target is fully aware of the DDW attack, removing the code makes it much harder for the target to determine how the virus was inserted and how to develop countermeasures against future attacks.

- Removing the DDW code makes it much more difficult for the target to determine the identity of the attacker, the determination of which could lead to serious legal or military sanctions against the attacker.

In some special cases, an attacker may want the code to revert back to the dormancy phase to await a future trigger and another attack. For example, malicious code in an exported anti-aircraft missile system may cause the missile to veer right and miss the target only when a certain signal is transmitted. To the DDW target, this looks like an isolated missile malfunction and he may elect to keep the system in operation without discovering the true reason for the malfunction. The missile system would work well during all tests and in use against aircraft that do not transmit that certain signal but the DDW attacker would know that his aircraft are safe from that missile system.

Putting the code back into dormancy is risky, however, since the attacker has no way of knowing whether the target will have detected the code when the next attack is triggered. The target could be preparing countermeasures or, perhaps, figuring out a way to use the code against the attacker. The reasons listed above for why it is wise to remove the code also serve to underscore the risks of sending it back to dormancy. Only when penetration is extremely difficult and the risk of counterdetection is less important should this be considered.

Predictability - The Common Denominator in All DDW Attacks

The one aspect of DDW that must remain a constant throughout the attack is the necessity for the attacker to accurately predict what the code will do. One obvious reason, of course, is that unpredictable code may not achieve the objectives the attacker set out to accomplish. The very definition of DDW is based on the premise that the attack is targeted against a specific system for a specific reason. Code that is unpredictable in its application and outcome cannot meet the requirements of DDW. Therefore, in this sense, predictability is critical when discussing DDW.

Another reason that predictability is important is common to all weapons. The old saw that "he who lives by the sword, dies by the sword" has never been more true than it is today when discussing DDW. When the US Army contracted a study to determine the feasibility of developing DDW-type viruses for military use,[16] many people had misgivings that were summed up by Gary Chapman, program director of Computer Professionals for Social Responsibility. "Unleashing this kind of thing is dangerous," he said. "Should the virus escape, the United States heads the list of vulnerable countries. Our computers are by far the most networked."[17] Less alarmist, Cramer and Pratt agree. They say that if viruses are to be practical, they need to be predictable.[18] Any weapon must be able to be armed and disarmed. It must be targetable and not endanger the army the wields it.[19] Developers of DDW should, in general, co-develop a detection and immunization program for all viruses they intend to use. In this way, a DDW attack gone wrong cannot inadvertently do harm to the attacker. In short, users and developers of DDW need be aware of the risks and the absolute requirement for predictability when developing DDW code.

---

[16]Richards, Evelyn. "Army Scouting to Enlist Aid of Computer Virus." The Washington Post 23 May 1990, Page C1.
[17]Shulman, Seth. "(Artificial) Germ Warfare." Technology Review October 1991, 19.
[18]Cramer, 76.
[19]Shulman, 19.

DDW and the Levels of Warfare

Wyatt Cook asserts that information warfare can be used at all three levels of war--tactical, operational and strategic.[20] He argues that at the strategic level, which focuses on the overall war effort, the most effective use of information warfare is to terminate conflict before conventional forces are ever employed. At the operational level, information warfare should exploit the military information systems and disrupt them to prevent the effective use of information by the enemy commander and his chain of command. Finally, the tactical employment of information warfare should be to isolate the enemy tactical forces from its leadership. Using this as a framework, it can be shown that DDW is useful in meeting tactical, operational and strategic objectives.

At the tactical level, DDW can target a specific weapon system or communications device, making the enemy soldier less effective and cutting him off from his chain of command. Operationally, DDW can disrupt C4I systems used by the theater commander to prosecute the war effort. At the strategic level, DDW can destroy the entire digital infrastructure of a nation, bringing commerce to a halt while instilling fear and uncertainty in the populace. This could force a nation to make concessions without a conventional armed attack. Table 3, on the following page, gives some examples of how DDW can be used in the different levels of warfare:

[20]Cook, Wyatt C. "Information Warfare: A New Dimension in the Application of Air and Space Power." Research paper, Air War College, Maxwell AFB, 1994.

Warfare Level	Possible Target(s)	Immediate Objective	Overall Goal
Strategic	- National financial network - Private telecom networks - Stock exchanges - Air traffic control system	- Stop commerce - Create fear/uncertainty in populace	- Political-economic - Force targeted nation to comply with attacker's wishes
Operational	- Military C4I network - Regional power grid	- Severe comms links - Disable central computer systems	- Disrupt enemy commander's use of information and ability to communicate with political leaders and military commanders
Tactical	- Tactical nets - Specific weapon systems	- Severe comms links between other tactical units and commander - Make warfighting equipment unusable	- Target-specific concerns - Isolate enemy forces from chain of command - Soften enemy forces for conventional attack

Table 3 - Examples of how DDW can be used Strategically, Operationally and Tactically

Developing a Strategy for Employing DDW

Like any weapon system, DDW needs to be examined to see how it can best be utilized to meet national military strategy. To do this, three questions need to be asked:

Who should control the employment of DDW?

What type of systems should be targeted?

Under what circumstances should DDW be used?

Who Should Control the Employment of DDW?

There are a couple of ways to look at this question. First, consider the fact that when used strategically, the effects of DDW are no less devastating than those yielded by any weapon of mass destruction. As such, the use of DDW should be authorized only by the Commander-in-Chief or the Chairman of the Joint Chiefs of Staff. On the other hand, certain forms of DDW are sufficiently targetable and the results sufficiently contained that a CINC or Joint Task Force Commander should have the power to order the use of this weapon as the need arises and the opportunity presents itself. These positions are not mutually exclusive and both have some merit.

One of the unique qualities of DDW code is its ability to lie dormant for a long period of time before it is triggered. It then follows that there are often two decisions that need to be made. First is the decision to insert the code into the targeted system(s) and second, is the decision to trigger the code from its dormancy in order that it fulfill its mission component. The question of who should control the employment of DDW needs to be restated as two separate questions: "Who should make the decision to insert DDW code into a targeted system?" and "Who should control the decision to trigger the code, if the trigger is external to that system?"[21] To answer these questions, it helps to classify DDW into three categories.

Category 1 types of DDW are clearly strategic in nature and both the decisions to insert this type of code and trigger it must certainly be made at the highest levels of the government. Any DDW targeting whole economies or one designed to instill fear and uncertainty in a targeted country's populace falls in this category.

Category 2 types of DDW would be that designed to lay dormant for long periods of time, as future insurance, but have only operational or tactical application when triggered. This type of DDW may, in fact, never be activated. Specially designed circuit boards in critical exported equipment would fall into this category. The decision to insert special code that can be activated in the event equipment falls into the hands of a future belligerent must be made at the highest levels of government. The decision to trigger the code, however, should be made by the operational commander.

Category 3 DDW is that which is inserted just prior to use and whose application is operational or tactical in nature. For this type of DDW, the code is triggered as soon as friendly forces can best exploit the DDW attack. Also falling in this category are operational/tactical DDW attacks that have no external triggers or no dormancy periods at all. For this category of

[21]Clearly, if the DDW code is a logic bomb or code not designed to go into dormancy (that is, completely autonomous after insertion), the person making the decision to insert the code is also the person who determines that the code will be allowed to fulfill its designated mission.

DDW, the CINC or JTF commander should be the decision authority for both the insertion and use of DDW.

Type of DDW Code	Authority to Insert Code/ Authority to Use DDW for a Category of Targets	Authority to Trigger Code/ Authority to Use DDW in a Specific Instance
Strategic Application Any Dormancy Length (Category 1)	Commander-in-Chief	Commander-in-Chief Chairman, JCS
Operational/Tactical Application Long Periods of Dormancy (Category 2)	Commander-in-Chief Chairman, JCS	CINC JTF Commander
Operational/Tactical Application Short or no Dormancy (Category 3)	CINC JTF Commander	CINC JTF Commander

Table 4 - Who Should Control Employment of DDW?

What Type of Systems Should Be Targeted?

The type of systems vulnerable to DDW has been examined throughout this paper. In short, these include any systems:

- Which use digital code to collect, analyze, process, or disseminate information, and
- Which are vulnerable to the covert insertion of digital code.

When developing a strategy for the use of DDW, you need to consider which of these systems to target. From the political-military perspective of an attacker, it would be beneficial if nearly every system vulnerable to attack was, indeed, infected with DDW code that was unknown to the target and could be controlled by the attacker. From a practical standpoint, that would be impossible.

Instead, DDW targets must be prioritized in much the same way as targets for conventional forces.[22] Target sets must be composed after careful and extensive analysis of:

[22]These considerations are adapted from those used in air campaign targeting. Refer to: Shultz, Richard H. and Pfaltzgraff, Robert L. Jr. The Future of Air Power in the Aftermath of the Gulf War. Maxwell AFB: Air University Press, 1992: 24.

(1) The targeted system. What type of data does it process? How much is known about it and can DDW code be devised to exploit it? How will DDW code be inserted and what is the probability of counterdetection before its mission component is activated?

(2) The goal of the DDW attack. What is it meant to accomplish and what is the probability of success? What are the goals of the political leadership and what are the goals of the overall conflict (subject to ongoing reassessment)?

(3) The particular strengths and weaknesses of the enemy. How will this DDW attack exploit his vulnerabilities? Will he have backup systems available to handle the workload of those systems that are attacked? Can he accomplish his mission by means other than automated systems that are subject to DDW attack?

(4) The presumed modus operandi down to the tactical level. How will DDW affect the way the enemy carries out his mission? Is command and control centralized or decentralized? How will DDW contribute to the overall war effort?

Strategic forms of DDW need to be used in ways that ensure the result of the DDW attack furthers national policy goals. The targets appropriate for strategic level attack (see Table 3 above) are not appropriate for operational and tactical uses of DDW. Therefore the DDW target set is dependent on the level of warfare for which DDW is considered.

Most importantly, the military planner needs to ensure that the employment of DDW is used in concert with other forms of military power to best achieve the desired results. DDW is not the only tool available to military forces, but one that should be used in a coordinated manner with other weapons.

Under What Circumstances Should DDW Be Used?

This final question underscores the unique nature of digital data warfare. DDW can be used in distinctly different ways. It can be a highly accurate, "precision guided" weapon, lethal only to its intended target with little or no "collateral damage." An example is an EPROM inserted into fighter aircraft prior to export that would disable the flight control system when a

specific RF signal is transmitted or a virus inserted into the enemy's tactical net that would disrupt encrypted communications at a specific time. Used like this, DDW is the cyberspace equivalent of a high powered rifle, a guided munition or, perhaps, a cruise missile.

On the other hand, DDW can be used to cause widespread damage. A virus in the computer used to control a region's power grid would cause widespread havoc as critical military, civil and medical systems shut down. Dr. David H. Arnold argues that a country's financial network may be targeted as a center of gravity and that the disruption of a country's main financial communication nodes could have a "long term, devastating effect" on its economy.[23] It is not hard to see how a properly executed DDW attack on a nation's financial network could cause complete economic collapse and topple a regime. Used this way, DDW becomes the information warfare equivalent of a nuclear blast.

Another aspect of DDW is its absolute need for secrecy. If the enemy were alerted to its existence prior to the code being triggered, he could develop a countermeasure and eradicate the code from his system. In a worst case scenario, friendly forces could be caught in an ambush. For these reasons, DDW should have a special status and, perhaps, be a part of the special operations domain. That is, we should use DDW much like we use special operations forces--selectively, covertly and with a limited number of players.

When developing a strategy for the employment of DDW, one needs to ask the question "Should DDW be used?" To answer that, the following ought to be considered:

(1) Can DDW do the job? Are there conventional methods that could do it more easily, more completely or with better chances of success?

(2) What are the political and military repercussions if the DDW is counterdetected and the attacker is identified?

---

[23]Arnold, David H. "Economic Warfare: Targeting Financial Systems As Centers of gravity." Edited by Karl P. Magyar, Challenge and Response: Anticipating US Security Concerns. Maxwell AFB: Air University Press, 1994.

(3) What is the possibility of the DDW code spreading in an unpredictable manner? Could it have a far more devastating effect than anticipated? Is there a possibility that it could infect systems beyond the intended target(s)? Could it possibly infect friendly or neutral systems?

(4) While DDW always begins as a covert operation, what is the anticipated international political fallout if the attack became public?

(5) Will the exposure of one DDW attack give away DDW attacks underway but still not triggered? That is, if it becomes necessary to trigger a trojan horse resident in a certain type of gear that was delivered with the code embedded in a circuit board, will other recipients of that equipment suspect that their arms are also so infected?

Protection Against Digital Data Warfare

Thus far, we have looked at DDW from an attacker's point of view. Let us now consider some of the protective measures that can be taken to protect an organization from a DDW attack. First, it must be stated that there is no such thing as a perfectly secure system. According to Frederick B. Cohen, an expert in the field:

> "In every case we are aware of, attack is feasible given an attacker with physical access to the system, adequate tools for system debugging, and adequate knowledge and persistence. There is no perfect defense."[24]

There is no global model of virus detection available.[25] Therefore, we must develop a plan to prevent infection and, if infection is detected or suspected, have procedures for minimizing the impact of DDW to the system. In formulating an effective defense, it is useful to remember that a DDW attack is successful only if it is allowed to fulfill its mission component and, even then, only if the successful completion of its mission allows the attacker to meet his objectives. A DDW attack can be foiled at anytime during its lifecycle by eliminating or containing the malicious code. Moreover, even if the mission component is successfully executed, the DDW attack itself is not a success if the target is

[24]Cohen, Frederick B. "Defense-in-Depth Against Computer Viruses." Computers & Security 11 (1992): 578.
[25] Schwartau, Winn. "Information Terrorism Threatens Way of Life." InfoWorld 09 September 1991, S72.

prepared such that the resultant loss of information or equipment does not allow the attacker to meet his objectives. With this in mind, a robust DDW defense should incorporate five "barriers" to protect against successful attack:

Prevent Penetration - The first defensive barrier. Take measures to ensure DDW code cannot penetrate the system.

Detect/Eradicate - The second defensive barrier. Since it is impossible to ensure that DDW code will never enter the system, have a method to detect malicious code that has made it past the first barrier. Then, have a way to get rid of the code once it is detected, preferably before it has an opportunity to damage the system.

Prevent Propagation - The third defensive barrier. Have measures in place to contain the propagation of detected *and undetected* malicious computer code.

Recovery - The fourth defensive barrier. Have a way of restoring programs, data and hardware following a DDW attack.

Alternative Operations - The fifth and last defensive barrier. In the case where DDW is successful in making the system unusable, have a way to accomplish the mission without the disabled equipment.

Implementing The Defensive Barriers

Constructing the five defensive barriers entails adopting a combination of hardware, software and procedural measures. The more solidly the barriers are constructed, the less likely a DDW attack will be successful. There is a tradeoff, however, since rigid barriers make using the system more difficult for the users, complicate the system's design and often come at a cost to performance. Moreover, direct and indirect monetary costs will be greater for highly defended systems. Each organization needs to determine how rigid a specific system's defense will be by balancing the criticality of the system against the costs associated with the design and

implementation of the defensive barriers. The following outlines some hardware, software and procedural measures that can be taken to construct the five defensive barriers.[26]

Barrier One - Prevent Penetration

Use a surge protector and UPS for added protection against some back-door coupling techniques.

Provide shielding around critical systems.

Design your own systems. Be alert for the possibility of DDW code in pre-programmed circuit boards or PROMs if not produced in a trusted environment.

Isolate highly protected, critical systems from less protected nodes.

Use passwords to prevent unauthorized system access. Consider physical identification in the form of a key or ID card coupled with the password for greater security.

Restrict access through insecure communications lines.

Encrypt signals sent across potentially insecure communication paths.

Implement an audit system to see how workers are using informational resources. Be on guard for excessive attempts to access accounts or other resources that are protected.

Prevent user access to system software and data. Ensure that such software is fully protected and that appropriate monitoring is done to detect attempts at unauthorized access.[27]

Prohibit users from installing software. This is probably the easiest way for DDW to penetrate a system and is also the easiest to prevent. Several military computers used during the Persian Gulf war were infected, probably as a

[26]See Appendix II for summary table.

[27]Wack, John P. and Carnahan, Lisa J. "Virus Prevention for Multiuser Computers and Associated Networks." Rogue Programs: Viruses, Worms, and Trojan Horses. Ed. Lance J. Hoffman. New York: Van Nostrand Reinhold, 1990, 289.

result of running unauthorized software.[28] Fortunately, none of those computers were mission critical.

Implement the "Principle of Least Privilege" whereby you give the user of a computer system all the privileges he needs to do his job, but no more.

Limit physical access. Consider installing biometric identification devices (for identification based on a fingerprint, a retinal scan, or a facial infrared imaging) as a means of stronger authentication before physical access to certain critical areas can be obtained.

Train users in malicious code penetration techniques.

Test the physical security of the system on a regular, unpredictable basis.

Test the electronic security of the system with a penetration analysis.[29]

Barrier Two - Detect/Eradicate

Install circuit breakers designed to detect unusual clock speeds or thermal stress and shut off power to equipment prior to damage occurring.

Use scanning and immunization software to detect and prevent infection from viruses and, once detected, eradicate them.

Track CPU cycles to see if CPU usage is greater than can be accounted for with known tasks.

Use cryptologically strong checksums.

Train users in malicious code detection and prevention techniques.

Barrier Three - Prevent Propagation

Install PROMs/CD-ROMs to prevent modification of executable programs.

Install special PC boards that attach to the hard disk controller and prevent modification of programs or startup areas on the hard disk.

---

[28]Husted, Bill. "Computer Viruses Carry Threat to U.S. Security. Military Admits Its Systems Infected." Atlanta Constitution 23 November 1991, Page A1.

[29]Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway (New York: Thunder's Mouth Press, 1994), 374.

Use different processor types throughout the system with different instruction sets making the DDW code's job of propagation much more difficult.

Use several different operating systems throughout the system to decrease virus propagation potential.

Isolate system if virus is detected.

Barrier Four - Recovery

Backup often. Keep critical programs locked up.

Have alternative communication methods (digital and voice) in case primary and secondary means are unavailable.

Have a contingency plan available.

Establish DDW "swat teams," made up of the most technically knowledgeable people in the organization, ready to spring into action when there is any indication of a DDW attack.

Barrier Five - Alternative Operations

Have other equipment available that is capable of performing the function of the disabled equipment.

If a whole system is involved, have a "hot site" (a complete, fully functioning ADP facility) available where operations could be transferred. Ideally, this hot site should be isolated enough to ensure a DDW attack at the primary site would not affect the hot site prior to detection.

In testimony before the House Sub-committee on Criminal Justice, Raymond Krammer, then deputy director of the NIST, made a statement concerning computer viruses that holds true when discussing DDW. He said, "...viruses must be addressed as part of an overall information

security program, and the problem itself must be attacked on several fronts--through a combination of technical mechanisms, users' awareness and good management."[30]

Building an Organization to Defeat DDW

While DDW does not only attack computer systems (it can attack any piece of equipment that uses a digital processor), it is the computer networks and communications nodes that are the most vulnerable to DDW. Therefore, it is crucial that every organization that operates a computer system and uses that system to process mission critical data take steps to ensure that its vulnerability to DDW is minimized.

System security is not a technology. It is an attitude; a state of mind. Operations and security are often in conflict. Operators want computer systems readily available and easy to use. Security measures often dictate restricted usage and cumbersome validation procedures. Security measures often seem to get in the way and appear to contribute little to the "bottom line." While automated data processing is dedicated to creating greater access to more useful information, system security seems to want to restrict that access and reduce the flow of useful information. On the other hand, failure to defend against a DDW attack could mean the loss of information or the deprivation of critical systems that could, in turn, spell the loss of the organization and its people or, at the very least, the inability of that organization to perform its mission.

Proactive management is the key to system security in a DDW environment. A system security program should consist of required actions to assure an acceptable degree of security for a computer system. While OMB circula A-130 outlines the minimum security requirements for federal automated information systems, its requirements are not stringent enough to deter most information warriors. It certainly would not significantly hinder a DDW attack from a determined foe.

---

[30]Krammer, Raymond G. "Defending Against Virus Attacks." Security Management 34.5 (1990): 37.

Every system manager needs to have a methodology to identify system vulnerabilities to DDW and a plan for how to minimize those vulnerabilities. At the very least, a robust security program should include:

1) A systems security officer who has overall responsibility for the security program and has sufficient authority to enforce security policy. This person needs to be knowledgeable in information technology and security matters. Additionally, this person needs to know how information systems are used within the organization by the people on the job.

2) Written security policy and a security plan to tell how to provide for security under normal operations. The policy should be flexible, broad level, and include training. The security plan would include system information, sensitivity of information and system security measures (the key part of the plan!). This policy must be backed up by a realistic budget.

3) Risk analysis program that would minutely examine system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

4) Continuity of Operations Plan. This will allow the organization to continue operations in the event of a DDW attack. This would include:

- An emergency action plan to delineate emergency responses to DDW while the attack is actually underway. The goal of the emergency action plan is to protect lives, limit damage and minimize impact on operations.
- A backup operations plan to ensure essential processing can be done after the attack. The goal is to provide all the information and documentation needed to restore the system.
- A disaster recovery plan to establish recovery procedures to restore full operational capabilities. The goal here is to resume full operations in a minimum amount of time.

5) Computer (or system) security awareness training to make users aware of threats and vulnerabilities.

In the end it must be said that there is no such thing as total computer security. You have to balance the risk against security with operational efficiency.

Conclusion

Digital Data Warfare is a discipline that is still very much in its infancy and which holds great promise for the person or organization that is able to overcome its many challenges. The US Army has recognized this and it appears some terrorist organizations are also investigating this method of warfare.[31]

DDW is cheaper than conventional warfare. A tiny piece of code can have the same effect on a city's power grid as a tomahawk missile. There are no large armies to field, no expensive fleets of ships, aircraft or armor.

DDW is covert. An attack can be made and the target left with no indication of its origin. A DDW attack can be made when other forms of aggression would be seen as unacceptable in the international arena. DDW code can be developed nearly anywhere without the need for big factories or R&D centers. DDW code can often be inserted into target systems remotely leaving no trace of the attacker.

DDW is customizable and scalable. DDW can be made to crash a fire control computer or bring down an entire economy. It can infect a single system or an entire network. It can make very small, almost insignificant changes to executable programs or it can completely destroy them.

DDW is technically feasible today. The pool of persons with the technical ability to develop DDW-type code is steadily growing as computer literate children and teenagers reach adulthood. This presents us with an ever growing supply of information warriors from within but also an ever greater threat from without.

[31]Hruska, Jan. Computer Viruses and Anti-Virus Warfare. West Sussex: Ellis Horwood, 1990.

Persons designing mission critical systems must be cognizant of the threat presented by DDW and ensure countermeasures are built into the design and implementation of the system. DDW is the next generation weapon and we must all be prepared to meet its challenges.

Appendix I

Definition of Terms

Malicious computer code - Any computer code that is on a system without the consent of the owner.

Trojan Horse - Malicious computer code that is located within a desirable block of code (i.e., an application program, operating system software, etc.). To be a trojan horse, the presence of the code must be unknown and it must perform an act that is not expected by the owner of the system.

Computer Virus - Malicious computer code that attaches itself to another block of code in order to propagate. Viruses have the following components:

- Self propagating mechanism. Must be able to move from one part of a system to another. Unlike worms, viruses cannot propagate beyond the host system without being downloaded or inserted.
- Capability to replicate itself. A virus may not necessarily make copies of itself if it can fulfill its mission without replication, but it does have that ability.
- Mission component. Must <u>do</u> something (usually something bad from the perspective of the system's owner)
- Trigger. Must have a mechanism to set the virus off to do its mission.

Computer viruses begin their lives as trojan horses and some remain trojan horses throughout their existence.

Worm - Malicious computer code, similar to a virus, that can replicate itself. Worms are independent operating programs that can mail replicas of themselves outside the host system. Worms may or may not have a mission component or a trigger.

Logic Bomb - A type of trojan horse that may or may not be a virus. Its mission component is triggered by a true/false condition. Logic bombs do not propagate; they just sit and wait.

Time Bomb - A subset of the logic bomb; its trigger is the date and/or time.

Trap Door - A hidden software mechanism triggered to circumvent system security measures. This can be a legitimate programming technique that allows a developer to bypass lengthy log-on routines or access source code directly. Its existence, if known by unauthorized persons, however, can be the source of a significant security breech.

Flying Dutchman - A trojan horse that erases all traces of itself after performing its mission. This is a common feature of trojan horses that helps defeat subsequent investigation.

Appendix II

Defensive Barriers Against a Successful DDW Attack

	Hardware Measures	Software Measures	Procedural Measures
Barrier One Prevent Penetration	- Surge protector/UPS - Shield critical systems - Design own systems - Isolate critical systems	- Use passwords - Restrict access through insecure comm lines - Encrypt signals sent through insecure comm lines - Implement audit system - Restrict access to system software and data - Restrict s/w installation authority	- Implement Principle of Least Privilege - Limit physical access - Train users in DDW penetration techniques - Test physical security - Test electronic security
Barrier Two Detect/Eradicate	- Install breakers to shutdown system when design limits are exceeded	- Use scanning/ immunization software - Track CPU usage - Use checksums	- Train users in malicious code detection and prevention methods
Barrier Three Prevent Propagation	- Install PROMs/CD-ROMs where feasible - Install h/w to prevent s/w access to certain parts of the system - Install different processors throughout the system	- Use different operating systems throughout the system	- Isolate system if malicious code is detected
Barrier Four Recovery			- Backup often - Keep critical programs locked up - Have alternative comms methods - Have contingency plans - DDW "swat team"
Barrier Five Alternative Operations			- Backup equipment - "Hot Site"

Bibliography

Alexander, Michael. "Military Sees Problems, Promise in Viral Strikes." Computerworld 08 April 1991, 97.

------. "Poor Security Made DoD Easy Hacker Prey." Computerworld 25 November 1991, 92.

Anthes, Gary H. "Info-terrorist Threat is Growing." Computerworld 30 January 1995.

Arnold, David H. "Economic Warfare: Targeting Financial Systems As Centers of gravity." Edited by Karl P. Magyar, Challenge and Response: Anticipating US Security Concerns. Maxwell AFB: Air University Press, 1994.

Arquilla, John and Ronfeldt, David. "Cyberwar is Coming!" 1992(?) Air University Library, Maxwell AFB, Alabama.

Campbell, Douglas. "Computer Contagion." Security Management 32.10 (1988): 83-84.

Carrol, John M. Computer Security. 2nd ed. Butterworth-Heinemann: Stoneham, 1987.

Cohen, Frederick B. "Defense-in-Depth Against Computer Viruses." Computers & Security 11 (1992): 563-579.

Cook, Wyatt C. "Information Warfare: A New Dimension in the Application of Air and Space Power." Research paper, Air War College, 1994.

Cooper, Pat. "In Cyberspace, U.S. Confronts An Illusive Foe." Defense News 10 (February 13-19, 1995): 1, 37.

Cramer, Myron L. and Pratt, Stephen R. "Computer Virus Countermeasures - A New Type of EW." Defense Electronics October 1989, 75-85.

Dehaven, John. "Stealth Virus Attacks." Byte 18.6 (1993): 137-142.

DiDio, Laura. "A Menace to Society." Network World 06 February 1989, 70-71, 82-85.

Fisher, Sharon. "The Internet Worm Celebrates Its First Birthday." InfoWorld 23 October 1989, S10-S12.

Gantz, John. "Meta-Virus Set to Unleash Plague on Windows 3.0 Users." InfoWorld 01 April 1991, 39.

Garreau, Joel. "Treasury Told Computer Virus Secrets: Whistleblowers Halted Display Available to Anyone With a Modem." The Washington Post 19 June 1993. Page A1.

Gunther, Judith, Kantra, Suzanne and Langreth, Robert. "The Digital Warrior." Popular Science September 1994, 60-64, 89.

Hruska, Jan. Computer Viruses and Anti-Virus Warfare. West Sussex: Ellis Horwood, 1990.

Husted, Bill. "Computer Viruses Carry Threat to U.S. Security. Military Admits Its Systems Infected." Atlanta Constitution 23 November 1991, Page A1.

Hutcherson, Norman B. "Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base." Research Report AU-ARI-94-1, Air University, September 1994.

Jenish, D'Arcy. "A 'Terrorist' Virus." Maclean's 16 March 1992, 48-51.

Kabay, Michel. "Information Warfare Could Be More Than Fiction." Network World 06 September 1993, 32.

Krammer, Raymond G. "Defending Against Virus Attacks." Security Management 34.5 (1990): 37-38.

Lewyn, Mark. "'Killer' Computer Viruses: An Idea Whose Time Shouldn't Come." Business Week 23 July 1990, 30.

Madsen, Wayne. "Government-Sponsored Computer Warfare and Sabotage." Computers & Security 11.3 (1992): 233-236.

McConnell, Robert. "Malicious Computer Code Electronic Warfare." Intelligencer May 1993, 12.

O'Malley, Christopher. "Stalking Stealth Viruses." Popular Science 242.1 (1993): 54-58.

Pine, Art. "Pentagon Looks to Start High-Tech Revolution in Ways of War." Los Angeles Times, 27 July 1994, Home Ed., 5(A).

Preston, Charles. "Creating a Corporate Virus Plan." Computers & Security 10.8 (1991): 701-710.

Richards, Evelyn. "Army Scouting to Enlist Aid of Computer Virus." The Washington Post 23 May 1990, Page C1.

Shultz, Richard H. and Pfaltzgraff, Robert L. Jr. The Future of Air Power in the Aftermath of the Gulf War. Maxwell AFB: Air University Press, 1992.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway New York: Thunder's Mouth Press, 1994.

------. "Fighting Terminal Terrorism." Computerworld 28 January 1991, 23.

------. "Information Terrorism Threatens Way of Life." InfoWorld 09 September 1991, S72-S73.

Shulman, Seth. "(Artificial) Germ Warfare." Technology Review October 1991, 18-19.

"The Gulf War Flu." U.S. News & World Report 20 January 1992, 50.

Wack, John P. and Carnahan, Lisa J. "Virus Prevention in General." Rogue Programs: Viruses, Worms, and Trojan Horses. Ed. Lance J. Hoffman. New York: Van Nostrand Reinhold, 1990. 43-49.

------. "Virus Prevention for Multiuser Computers and Associated Networks." Rogue Programs: Viruses, Worms, and Trojan Horses. Ed. Lance J. Hoffman. New York: Van Nostrand Reinhold, 1990. 287-294.

Wilson, David L. "'Crackers': a Serious Threat." The Chronicle of Higher Education. 40 (August 17, 1994): A23-A24.